



BULLETIN DE SECURITE

Titre	Vulnérabilités affectant le navigateur Mozilla Firefox
Numéro de Référence	63412204/26
Date de publication	22 avril 2026
Risque	Important
Impact	Important

Systemes affectés

- Mozilla Firefox versions antérieures à la version 150
- Mozilla Firefox ESR versions antérieures aux versions 115.35 et 140.10

Identificateurs externes

CVE-2026-6746	CVE-2026-6747	CVE-2026-6748	CVE-2026-6749	CVE-2026-6750
CVE-2026-6751	CVE-2026-6752	CVE-2026-6753	CVE-2026-6754	CVE-2026-6755
CVE-2026-6756	CVE-2026-6757	CVE-2026-6758	CVE-2026-6759	CVE-2026-6760
CVE-2026-2781	CVE-2026-6761	CVE-2026-6762	CVE-2026-6763	CVE-2026-6764
CVE-2026-6765	CVE-2026-6766	CVE-2026-6767	CVE-2026-6768	CVE-2026-6769
CVE-2026-6770	CVE-2026-6771	CVE-2026-6772	CVE-2026-6773	CVE-2026-6774
CVE-2026-6775	CVE-2026-6776	CVE-2026-6777	CVE-2026-6778	CVE-2026-6779
CVE-2026-6780	CVE-2026-6781	CVE-2026-6782	CVE-2026-6783	CVE-2026-6784
CVE-2026-6785	CVE-2026-6786			

Bilan de la vulnérabilité

Mozilla Foundation annonce la disponibilité d'une mise à jour de sécurité permettant la correction de plusieurs vulnérabilités au niveau du navigateur Mozilla Firefox. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code à distance, d'accéder à des informations confidentielles, de contourner des mesures de sécurité, d'élever ses privilèges ou de causer un déni de service.

Solution

Veillez se référer aux bulletins de sécurité Mozilla afin d'installer les nouvelles mises à jour.

Risques

- Exécution de code à distance
- Accès à des informations confidentielles
- Contournement de mesures de sécurité
- Elévation de privilèges
- Déni de service

Références

Bulletins de sécurité Mozilla:

- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-30/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-31/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-32/>